ABSTRACT OF THE DISCLOSURE

A technique for generating a strong random number for use in a cryptographic security system for a processor-based device is provided. The technique is particularly useful for restoring a random number to memory after data in the memory has been lost due to, for example, loss of backup power. Bits comprising a random number are automatically and iteratively written to the memory when another authorized device or application program attempts to access the processor-based device. Further randomness also may be provided by masking in additional bits whenever main power is cycled to the processor-based device.